

WHAT IS CLAIMED IS:

- Sub A4*
- 5
1. A public key authorization infrastructure comprising:
a client program accessible by a user;
an application program;
a certificate authority issuing a long-term public key identity certificate
(long-term certificate) that binds a public key of the user to long-term
identification information related to the user;
a directory for storing short-term authorization information related to the
10 user; and
a credentials server for issuing a short-term public key credential
certificate (short-term certificate) to the client, the short-term certificate binds
the public key of the user to the long-term identification information related to
the user from the long term certificate and to the short-term authorization
15 information related to the user from the directory, wherein the client program
presents the short-term certificate to the application program for authorization
and demonstrates that the user has knowledge of a private key corresponding to
the public key in the short-term certificate.
- 20 2. The public key authorization infrastructure of claim 1 wherein the short-
term certificate includes an expiration date/time.
- 25 3. The public key authorization infrastructure of claim 2 wherein a validity
period from when the credentials server issues the short-term certificate to the
expiration date/time is sufficiently short such that the short-term certificate does
not need to be subject to revocation.
- 30 4. The public key authorization infrastructure of claim 2 further comprising:
includes a certificate revocation list (CRL), wherein the expiration
date/time of the short-term certificate is no later than a date/time at which a next
CRL is scheduled.

5. The public key authorization infrastructure of claim 2 wherein the short-term certificate is not subject to revocation.
- 5 6. The public key authorization infrastructure of claim 1 wherein the short-term certificate is a non-structured short-term certificate.
7. The public key authorization infrastructure of claim 1 further comprising:
10 a second application program; and
wherein the short-term certificate is a structured short-term certificate
including:
15 a first folder corresponding to the first named application program
and containing long-term information and short-term information as
required by the first named application program;
a second folder corresponding to the second application program
and containing long-term information and short-term information as
required by the second application;
wherein the first folder is open and the second folder is closed
when the client presents the short-term certificate to the first named
20 application program for authorization, wherein closing the second folder
makes its contents not readable by the first named application program;
and
wherein the first folder is closed and the second folder is open
when the client presents the short-term certificate to the second
application program for authorization, wherein closing the first folder
25 makes its contents not readable by the second application program.
8. The public key authorization infrastructure of claim 1 wherein the short-term certificate is an X.509v3 certificate.
- 30

- 50
55
60
65
70
75
80
85
90
95
100
9. The public key authorization infrastructure of claim 7 wherein the first folder and the second folder are implemented as extension fields of an X.509v3 certificate.
- 5 10. The public key authorization infrastructure of claim 1 wherein the directory further stores the issued long-term certificate.
11. The public key authorization infrastructure of claim 1 wherein the private key is stored in a smartcard accessible by the client program.
- 10 12. The public key authorization infrastructure of claim 1 wherein the private key is stored in a secure software wallet accessible by the client program.
13. A method of authorizing a user, the method comprising the steps of:
15 issuing a long-term public key identity certificate (long-term certificate) that binds a public key of the user to long-term identification information related to the user;
storing short-term authorization information related to the user;
issuing a short-term public key credential certificate (short-term
20 certificate) that binds the public key of the user to the long-term identification information related to the user contained in the long-term certificate and to the short-term authorization information related to the user; and
presenting the short-term certificate on behalf of the user to an application program for authorization and demonstrating that the user has
25 knowledge of a private key corresponding to the public key in the short-term certificate.
14. The method of claim 13 wherein the short-term certificate includes an expiration date/time.
- 30

15. The method of claim 14 wherein a validity period from when the short-term certificate is issued to the expiration date/time is sufficiently short such that the short-term certificate does not need to be subject to revocation.

5 16. The method of claim 14 further comprising the step of:
maintaining a certificate revocation list (CRL), wherein the expiration
date/time of the short-term certificate is no later than a time at which the next
CRL is scheduled.

10 17. The method of claim 14 wherein the short-term certificate is not subject
to revocation.

18. The method of claim 13 wherein the short-term certificate is a non-structured short-term certificate.

15 19. The method of claim 13 wherein the short-term certificate is a structured
short-term certificate including a first folder corresponding to the first named
application program and containing long-term information and short-term
information as required by the first named application program, and including a
20 second folder corresponding to a second application program and containing
long-term information and short-term information as required by the second
application, wherein the method further comprises the steps of:

25 closing the second folder and leaving the first folder open prior to
the presenting step if the presenting step presents the short-term
certificate to the first named application program for authorization,
wherein closing the second folder makes its contents not readable by the
first named application program; and

closing the first folder and leaving the second folder open prior to the presenting step if the presenting step presents the short-term certificate to the second application program for authorization, wherein

closing the first folder makes its contents not readable by the second application program.

20. The method of claim 13 wherein the short-term certificate is an X.509v3
5 certificate.

21. The method of claim 19 wherein the first folder and the second folder are implemented as extension fields of an X.509v3 certificate.

10 22. The method of claim 13 wherein the method further comprises the step
of:
storing the issued long-term certificate in a directory.

15 23. The method of claim 13 further comprising the step of:
storing the private key in a smartcard.

24. The method of claim 13 further comprising the step of:
storing the private key in a secure software wallet.